USAWC STRATEGY RESEARCH PROJECT

PROTECTING AMERICA'S CRITICAL INFRASTRUCTURE: MAKING OUR PROGRAM MORE EFFECTIVE

by

Colonel Christopher Martin
United States Army

Dr. Antulio Echevarria
Project Adviser

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
15 MAR 2006		

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Protecting America's Critical Infrastructure Making Our Program More Effective	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Christopher Martin	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**28**	

ABSTRACT

AUTHOR: Colonel Christopher Martin

TITLE: Protecting America's Critical Infrastructure: Making Our Program More Effective

FORMAT: Strategy Research Project

DATE: 15 March 2006 WORD COUNT: 7,789 PAGES: 28

KEY TERMS: Critical Infrastructure Protection, Terrorism, Homeland Defense, Homeland Security

CLASSIFICATION: Unclassified

Critical Infrastructure in the U.S. is defined by the Patriot Act of 2001 as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." We are challenged to protect our critical infrastructure from attacks by terrorists and from natural disasters for a variety of reasons. A contributing reason for inefficiencies is the way the current program as established by Presidential Directive 7 (2003) assigns responsibilities. Initially I will address the definition of critical infrastructure and attempt to determine if this definition is adequate, and then move to an examination of our current program to see if there are ways to gain efficiencies and effectiveness. I will also determine if there is a common method to analyze critical infrastructure – i.e., vulnerability, risk, and cost-benefit analysis – to determine how we should prioritize funding for critical infrastructure protection. Finally, recommendations are provided to make our critical infrastructure program more effective.

PROTECTING AMERICA'S CRITICAL INFRASTRUCTURE: MAKING OUR PROGRAM MORE EFFECTIVE

> The basic nature of our free society greatly enables terrorist operations and tactics, while, at the same time, hinders our ability to protect, prevent, or mitigate the effects of terrorist acts.[1]

Protecting our critical resources from physical attack is a daunting task. The sheer number of facilities, icons, monuments, and buildings we consider to be critical virtually guarantees that much of our infrastructure is poorly protected at best. Despite the guidance in numerous documents, e.g., The Homeland Security Act of 2002, The National Strategy for Homeland Security, The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, and Homeland Security Presidential Directive – 7 (HSPD-7), there still does not appear to be an orchestrated program in the Unites States for protecting our infrastructure from future terror attacks. Compounding the problem even further, up to 85% of our critical infrastructure is privately owned with very little government oversight to secure those facilities.[2]

We are challenged to protect our critical infrastructure from attack by terrorists for a variety of reasons, to include inefficiencies in the way the current program is established, the administration of the critical infrastructure protection program, the very definition of critical infrastructure, and the overall allocation of scarce resources to implement protective measures. Also contributing to the inefficiencies of the program is our lack of understanding of the terrorist threat, and our corresponding inability to assess vulnerabilities and determine the risk involved if a facility is not protected or only protected to a certain level. This is not to say our critical infrastructure protection program is not effective -- indeed it is a successful component of our strategy of an active, layered defense to defeat terrorism– however its effectiveness could be significantly greater if the changes recommended in this paper were made.

We should expect terrorists to strike again in the United States. It is imperative we take those steps necessary to deter their efforts, disrupt their plans, and decrease their effectiveness where possible. Our critical infrastructure must be protected from attack because of the potential global impact of the destruction of systems in our country. The Interim National Infrastructure Protection Plan stated it very succinctly:

> Protecting our Nation's critical infrastructure and key resources (CI/KR) is vital to our national security, economic vitality, and way of life. Attacks on critical infrastructure could disrupt the direct functioning of key business and government activities, facilities, and systems, as well as have cascading effects throughout the Nation's economy and society. Furthermore, direct attacks on individual key assets could result not only in large-scale human casualties and property destruction, but also in profound damage to national prestige, morale, and confidence.[3]

The Threat

It is a reasonable assumption that terrorists will once again strike on U.S. soil, and therefore prudent that we plan accordingly, both in protection and in response. As we continue to promote positive change in Afghanistan and Iraq, Al-Qaeda's goal of establishing an Islamic caliphate is significantly hampered and the probability of another attack on the U.S. Homeland likely rises.

> The proliferation of WMD also is a concern as we determine what facilities to protect. Presently, at least twenty-four countries have or are pursuing WMD. By the turn of the century, twenty or more developing countries could acquire ballistic missiles, at least nine could have nuclear weapons, thirty or more could have chemical weapons, and ten could maintain biological weapons.[4]

While we are most likely to consider the threat of terrorism our primary concern for protecting critical infrastructure, as the recent hurricanes in Louisiana, Alabama, Florida, and Texas remind us, the threat can also be a natural disaster. How we protect our critical infrastructure from natural disasters and then react to damages if they occur may be used as indicators for the enemy as he develops his plans for the next attack on the Homeland. This is particularly true if the enemy determines he wants to conduct follow-on attacks on first responders. Therefore, it is imperative that we consider a variety of potential terrorist attack methods and natural disaster consequences that we use as a baseline in the design of new facilities, and in determining the requirements of hardening an existing facility. For instance, potential terrorist attack methods may include nuclear weapons, chemical or biological weapons, radiological weapons (dirty bombs), suicide bomber, hostage taking, vehicle borne improvised explosive device (truck bomb), or small improvised explosive device (backpack explosive). Natural disaster threats include large earthquakes, hurricanes, and flooding. Of course, not every facility is subject to each threat. Better recognition of potential targets is needed – those that will lead to mass destruction or mass casualties, or those systems where the enemy can attack "the elements of power sustaining the international system."[5]

Critical Infrastructure Defined

Before examining the methods used to determine the vulnerability of a particular structure or facility, we first have to analyze the term *critical infrastructure*. The Patriot Act of 2001 establishes the guidelines for critical infrastructure that all subsequent legislation refers to:

> …the term `critical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"[6]

This is a broad definition of critical infrastructure, and does little to help in the identification of critical facilities or buildings, and does not establish any requirements for prioritization of protection of the assets. By this definition, would the Twin Towers in New York City have been considered critical infrastructure? The answer is yes, but not because of the significant loss of life. Rather, the World trade Centers were critical infrastructure because of the Wall Street backup data stored in the buildings; destruction of this could (and did to a degree) impact the economic well-being of the nation. A recent Rand Study introduces a somewhat different definition of critical infrastructure:

> Critical infrastructure refers to transportation and energy systems, defense installations, banking and financial assets, water supplies, chemical plants, food and agricultural resources, police and fire departments, hospitals and public health systems, government offices, and national symbols. In other words, critical infrastructure refers to those assets, systems, and functions so vital to the nation that their disruption or destruction would have a debilitating effect on our national security, economy, governance, public health and safety, and morale.[7]

The Rand definition is much broader that that in the Patriot Act, but again does little to help in defining the problem because of its width and breadth. The most critical term in each of the definitions is that of "*debilitating effect on our [national] security,"* but there are no metrics provided to determine what is debilitating. Therefore our approach is to try and protect as much as possible, knowing that in many cases, we are adequately protecting none. As of September 2004, there were over 1,700 facilities the Undersecretary for Information Analysis and Infrastructure Protection had identified for vulnerability assessments. This is out of a list of over 33,000 facilities in the U.S. infrastructure data base.[8]

Current U.S Policy

The Clinton Administration recognized the significance of critical infrastructure and its vulnerability to attack, issuing PDD-63 in May, 1998. This Presidential Directive called for cooperation between the public sector and the federal government to protect our infrastructure and established nine critical systems it considered "essential to the minimum operations of the economy and government."[9] These systems were divided into sectors with various lead agencies assigned to coordinate protective measures. The agencies were to "meet to coordinate the implementation of this directive under the auspices of a Critical Infrastructure Coordination Group (CICG), chaired by the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism."[10]

The Protection Challenge

Agriculture and Food 1,912,000 farms; 87,000 food-processing plants

Water 1,800 federal reservoirs; 1,600 municipal waste water facilities

Public Health 5,800 registered hospitals

Emergency Services 87,000 U.S. localities

Defense Industrial Base 250,000 firms in 215 distinct industries

Telecommunications 2 billion miles of cable

Energy
- *Electricity* 2,800 power plants;
- *Oil and Natural Gas* 300,000 producing sites

Transportation
- *Aviation* 5,000 public airports
- *Passenger Rail and Railroads* 120,000 miles of major railroads; 590,000 highway bridges
- *Pipelines* 2 million miles of pipelines
- *Maritime* 300 inland/costal ports
- *Mass Transit* 500 major urban public transit operators

Banking and Finance 26,600 FDIC insured institutions

Chemical Industry and Hazardous Materials 66,000 chemical plants

Postal and Shipping 137 million delivery sites

Key Assets
- *National Monuments and Icons* 5,800 historic buildings
- *Nuclear Power Plants* 104 commercial nuclear power plants
- *Dams* 80,000 dams
- *Government Facilities* 3,000 government owned/operated facilities
- *Commercial Assets* 460 skyscrapers

*These are approximate figures.

This chart copied directly from the Strategy for the Physical Protection of Critical Infrastructure and Key Assets

Table 1

The tragic incidents of 11 September, 2001, amplified tremendously the requirement to protect critical infrastructure; two pieces of legislation – the Patriot Act and the Homeland Security Act -- addressed the issue, followed closely by President Bush's issuance of HSPD-7. In February, 2003, the DHS published the National Strategy for the Protection of Critical Infrastructure and Key Assets, and followed this with the National Infrastructure Protection Plan in February 2005.

The responsibility for execution of the protection of our critical resources lies with the Department of Homeland Security. The Homeland Security Act of 2002 made the Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) Directorate responsible for critical infrastructure protection functions with a lead role for sharing information about terrorist incidents with the DHS and the federal government. HSPD -7 also assigned that responsibility to DHS and it is again amplified in The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets (CI/KA).

> As the cross-sector coordinator, DHS will also be responsible for the detailed refinement and implementation of the core elements of this Strategy. This charter includes building and maintaining a complete, current, and accurate assessment of national-level critical assets, systems, and functions, as well as assessing vulnerabilities and protective postures across the critical infrastructure sectors[11]

Key Acronyms used in Critical Infrastructure Protection:

CI – Critical infrastructure
CIP – Critical infrastructure protection
CI/KA – critical infrastructure / key assets
CI/KR -- critical infrastructure / key resources
IA/IP – Information analysis and Infrastructure protection
NIPP – National Infrastructure Protection Plan

Just as PDD-63 divided infrastructure up into sectors, HSPD-7 and the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets and the Interim National Infrastructure Protection Plan (NIPP) also categorize critical Infrastructure into sectors. A carryover from PDD-63 is the assignment of a lead government agency for each sector (key assets are not assigned a lead agency). The National Strategy addressed the thirteen sectors shown below.[12]

- Agriculture
- Food
- Water
- Public Health
- Emergency Services
- Government
- Defense Industrial Base
- Information and Telecommunications
- Energy
- Transportation
- Banking and Finance
- Chemical Industry and Hazardous Materials
- Postal and Shipping

The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets introduced us to a new term -- *key assets* -- which is defined as "…targets whose destruction could cause large-scale injury, death or destruction of property, and/or profoundly damage our national prestige, and confidence."[13] This term applies generally to our national monuments and icons and also appears in the interim NIPP, but as a subset of *key resources*, which the NIPP defines as "publicly or privately controlled resources essential to the minimal operations of

the economy and government."[14] The National Strategy for the Physical Protection of CI/KA goes on to list three objectives:[15]

> The first objective of this Strategy is to identify and assure the protection of those assets, systems, and functions that we deem most 'critical' in terms of national-level public health and safety, governance, economic and national security, and public confidence.
>
> The second major objective is to assure the protection of infrastructures and assets that face a specific, imminent threat.
>
> Hence, the third objective of the Strategy is to pursue collaborative measures and initiatives to assure the protection of other potential targets that may become attractive over time.

The Interim NIPP contains five goals supporting the National Strategy: [16]

1. Protect CI/KR against plausible and specific threats;
2. Long-term reduction of CI/KR vulnerabilities in a comprehensive and integrated manner;
3. Maximize efficient use of resources for infrastructure protection;
4. Build partnerships among Federal, State, local, tribal, international, and private sector stakeholders to implement CIP programs;
5. Continuously track and monitor national protection.

To facilitate compliance with HSPD directives and programs, The Office of Homeland Security offered grants in 2005 to "any state agency, department, commission, board, campus," [17]etc. that requested the money based on an established set of priorities.[18] Our strategy for protecting critical infrastructure is outlined, the plan to implement the strategy is specified, and the government grants money to execute the plan, and yet there is a level of management that fails to orchestrate the policies our government has established. The next section will analyze our policy and the implementation of that policy in the U.S.

Analysis of Current Policy

Protection of critical infrastructure is a generally passive defensive measure that in and of itself is not capable of defeating terrorist attacks. This does not mean it is inappropriate to attempt to protect critical infrastructure, rather, that protective measures are but one more layer of defense against the possibility of attack. Protecting our critical infrastructure dissuades terrorist attack because of the level of complexity it adds to the terrorist planning, thereby lowering the likelihood of success if attacked.

At first glance, it would seem the United States has a policy in place that should be capable of preventing future terrorist attacks on our most critical infrastructure. The policy defines critical infrastructure, assigns responsibility to coordinate protection activities, has a coherent strategy to effect protection, and a plan to implement the strategy. However, it is difficult to determine how we are doing in critical infrastructure protection, primarily for two reasons: the lack of an effective tracking system, and a lack of accountability for money appropriated by Congress to agencies to combat terrorism.[19] In a report released in January 2006, the GAO said:

> …supplements or updates in the national strategies that include governmentwide (sic) or national level performance measures (i.e., goals and measures to track progress of the numerous efforts by the federal, state, and local governments and private sector to combat terrorism) have not been issued. Without governmentwide goals and measures, the Administration has no effective means of articulating to Congress or the American people the federal government's progress as a whole, related to combating terrorism.[20]

In the absence of a prioritized list of critical infrastructure, lack of baseline protection requirements, no vulnerability assessment standards, and no clearly responsible program director, it is easy to see how we may not be getting the best value (protection) for our money. Couple this with the fact that the majority of our infrastructure is privately owned, with no incentives other than free market incentives to protect the asset, and the image of a program not being properly implemented begins to emerge, possibly increasing the likelihood of attack as well as the potential for damages if attacked.

There are numerous problems with our current policy despite the legislative and executive planning that has gone into it. Again, this is not an issue of inadequate policy, but one of improper implementation. The policy is in place, but our inability to execute it as specified results in misallocation of resources and facilities not hardened properly. What's even worse, we do not seem to have a good handle on what is being done. The problems with our implementation are described below.

The critical infrastructure protection process. The risk management framework identified in the NIPP consists of five steps:[21]

1. Identifying critical assets
2. Identifying and assessing vulnerabilities
3. Normalizing, analyzing, and prioritizing study results
4. Implementing protective programs

5. Measuring performance

These five steps, if executed correctly and at the right level of government, are meant to guide us to protect those assets which truly are required by the nation to continue to function. Notice the absence of analyzing risk, however, in this framework. A better way of analyzing assets and assessing their vulnerability follows:

> The basic steps of CIP consist of: identifying the critical infrastructures, determining the threats against those infrastructures, analyzing the vulnerabilities of threatened infrastructures, assessing the risks of degradation or loss of a critical infrastructure, and applying countermeasures where risk is unacceptable.[22]

This framework is more comprehensive than that offered in the NIPP and would ultimately lead to assets which are netter protected.

Inadequate definition of critical infrastructure and key assets. The United States must develop a much more cohesive strategy that properly identifies critical infrastructure and key assets, assesses vulnerability, accounts for risk, prioritizes assets, and then funds protective measures accordingly. The National Strategy for the Physical Protection of CI/KA recognizes this requirement, but does not establish the mechanisms to execute these tasks. Our primary issue is assessing that which is truly critical to the government's ability to function if attacked. There are no metrics assigned to the definition of "*a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."* Without metrics or more clear guidance, it is easy to justify placing more facilities on the critical infrastructure list than should be there. As one author very succinctly stated the issue:

> The current list of critical infrastructure is too expansive, including sectors that are not truly vital to the federal government's functioning. The federal government has a nested interest in only the energy, finance, telecommunications, and transportation sectors.[23]

This statement, while taking a more focused approach to classifying critical infrastructure, is not necessarily correct either as it still tends to look at sectors vice components within a sector. For instance, not every electrical substation in the U.S. is critical. A substation that provides power to Wall Street is critical, while one that provides power to a small rural town would not be. As a Congressional Research Study indicated in September, 2004:

> However, not every asset is as important as another. In order to focus assessment resources, all of the methodologies reviewed suggest that the assessment should focus on those assets judged to be most critical. Criticality is typically defined as a measure of the consequences associated with the loss or degradation of a particular asset. The more the loss of an asset threatens the

> survival or viability of its owners, of those located nearby, or of others who depend on it (including the nation as a whole), the more critical it becomes.[24]

The Congressional research Staff has conducted several studies on critical infrastructure protection, and concluded in a September 2004 report that,

> …the IA/IP should be able to tell Congress what criteria it used to select assets of National importance, the basic strategy it uses to determine which assets warrant additional protective measures, and by how much these measures could reduce the risk to the nation. It should also be able to tell how much these additional measures might cost.[25]

The recommendation has yet to be implemented, and in fact, DHS is actually compounding the problem of identifying and tracking critical infrastructure in its 2006 budget request by proposing the creation of the Targeted Infrastructure Protection Program. This new program, if approved, allocates $600 million in grants to state and local governments to help protect "critical" infrastructure for public transit agencies, railways, seaports, and energy facilities. Fifty million dollars of this amount is specifically earmarked for implementing the Buffer Zone Protection Plan through the office of State and Local Government Coordination and Preparedness.[26] The program highlights several problems in our critical infrastructure protection program, first and foremost which is no established CI identification program, unless one boldly assumes DHS is satisfied all national-level critical infrastructure is already adequately protected. The program also highlights the issue of who is in charge of CIP in the federal government, and the pitfalls of a one size fits all approach to protecting critical infrastructure, i.e., establishing buffer zones around facilities. Critical infrastructure protection is not a problem we can just throw money at and expect all will turn out well.

Vulnerability assessments not standardized. Once infrastructure assets have been identified as critical, a vulnerability assessment must be made. This is another area where guidance is lacking and, ultimately, the entire critical infrastructure program is affected. Specifically, the vulnerabilities to assess have not been made clear, and many organizations therefore use their own criteria. To adequately prepare our defenses to protect critical infrastructure, we essentially need to examine the vulnerability of the infrastructure, the risk of attack, the risk we incur if it is attacked, and then conduct a cost-benefit analysis to determine if the facility is worth protecting, or the amount of security we can buy above the baseline level for a given amount of money. While this last concept is a cold-hearted view, it is the only way to determine a priority for defending our critical infrastructure. Standardized analysis tools must be used that examine the threat, vulnerability, and risk of the CI. The Interim National Infrastructure Protection Plan, published in February 2005, defines vulnerabilities as, "the

characteristics of an asset's design, location, or operation/use that render it susceptible to damage, destruction, or incapacitation by terrorist or other intentional acts, mechanical failures, and natural hazards."[27] The NIPP states it is "…based upon a risk management framework that takes into account threats, vulnerabilities, and consequences…," but the document fails to provide a methodology for making assessments of these critical factors.[28]

The result of there being no standard assessment methodologies is that every agency must develop their own methods to examine the vulnerability of their assets. One method in use is shown below:

> API/NPRA identifies three steps to assessing vulnerabilities: 1) determine how an adversary could carry out a specific kind of attack against a specific asset (or group of assets); 2) evaluate existing countermeasures for their reliability and their effectiveness to deter, detect, or delay the specific attack; and 3) estimate current state of vulnerability and assign it a value.[29]

This type of methodology is relatively easy to apply, assuming the user understands the threat and applies it properly. It is important that some consistent methodology be applied to assessing vulnerability so that informed decisions about how to apply scarce resources, specifically money, can be made.

Lack of a defined baseline level of protection. The IA/IP has not done an adequate job of identifying the baseline protection level all critical infrastructure assets should attain. Once we have identified critical infrastructure, we should develop a baseline level of protection we expect the facility to attain. This doesn't mean a facility that does not impact systems critical to the nation's ability to function are not important, it merely means we subjugate them to a lower level of protection. It also does not mean we do nothing about these lesser important facilities; they require at least a baseline level of protection. A key government agency, such as the Department of State, must protect its facilities from the effects of a large truck-type bomb, from suicide bombers attempting to enter the facility or mingle with lines outside it, and from the injection of a chemical or biological agent into its ventilation system, while an electrical substation feeding a major hospital may just require a fence around it. The substation's value to the hospital staff and patients is high, but its value to the nation is relatively low, and the protection level does not have to be of the same degree as does a State Department building.

There is an inherent value to providing protection to a facility or asset – an obviously protected target presents an image to terrorists that ultimately may deter them from attacking. Even baseline protection measures may impact the motivation of the terrorists as well as limit their ability to conduct an attack.

> The likelihood of an attack is a function of at least two parameters: a) whether or not the asset represents a tempting target based on the goals and motivation of the adversary (i.e. would a successful attack on that asset further the goals and objectives of the attacker); and, b) whether the adversary has the capability to attack the asset by various methods…. The asset's vulnerability to various methods of attack (determined in the next step) may also affect the attractiveness of the asset as a target.[30]

We do not have a mechanism in place to assess how effectively CI is protected, and there is no method to establish accountability for baseline protection levels. DHS, specifically the IA/IP, must provide guidelines to other agencies, state and local governments, and the private sector on minimum levels of protection required to keep critical infrastructure safe from attack. Without this guidance, our strategy to defeat terrorism is flawed – a layer of defense is missing.

> Governmentwide (sic) combating terrorism performance measures that support the national strategies would allow the Administration and Congress to more effectively assess the federal government's progress in combating terrorism initiatives, and better determine how effectively the government is using valuable resources. Furthermore, they would provide a more effective means of holding agencies accountable for achieving results.[31]

No established risk levels. Just understanding the vulnerability of an asset or facility is not enough. We also need a structured risk level analysis to determine what is acceptable and what is not. When conducting risk analysis, Kochems states, "There are two categories of risk: risks with thinkable consequences and those with unthinkable consequences."[32] We do not have a definition for either of these so far. There are no metrics corresponding to risk. Questions such as how many hours of lost electrical power are required for it to be debilitating to the government, or how many people must die before an event is considered catastrophic, must be addressed. Established risk levels determine how much protection above the baseline is required.

> The risk associated with a specific attack on an asset can be reduced by reducing the level of threat to it, by reducing its vulnerability to that threat, or by reducing the consequences or impact of an attack should it happen.[33]

Risk levels cannot focus solely on the immediate impact of the incident; rather, long term effects must be considered.

> While the immediate impact is important, so, too, is the amount of time and resources required to replace the lost capability. If losing the asset results in a large immediate disruption, but the asset can be replaced quickly and cheaply, or there are cost-effective substitutes, the total consequence may not be so great. Alternatively, the loss of an asset resulting in a small immediate consequence, but which continues for a long period of time because of the difficulty in reconstituting the lost capability, may result in a much greater total loss.[34]

There must be some established risk levels for protection so that the cost of protective measures does not exceed the value of the asset. As vulnerabilities are assessed, the damages that occur must be quantified in terms that help us determine the risk to the asset. The level of damage has to include more than just the physical damage to the infrastructure facility, it must also take into account the impact on other systems, and it must do so in quantifiable terms, such as lives lost, days of service impacted, impact on the economy, or damage to the environment, etc.

> Risk can be measured quantitatively, as shown below:
>
> Expected loss = (consequence) x (probability that an attack will occur) x (conditional probability that the attacker will use a specific method ((i.e. truck bomb)) x (the conditional probability that the attack will be successful)[35]

Risk can also be measured qualitatively:

> Risk is often measured qualitatively (e.g. high, medium, low). Since consequences may be measured along a number of different vectors, and threat and vulnerability have been measured separately, a qualitative measure of risk must have some criteria for integrating the number of different qualitative measures. For example, how should the assessment decide what risk rating to give a medium threat against a highly vulnerable target that would have a low death/injury impact, a medium environmental impact, but a high short-term financial impact? Does this scenario equal a high, medium, or low level of risk?[36]

Regardless of the method used (qualitative or quantitative), there must be some established level of acceptable risk to compare to so that priorities can be set and resources allocated, where required, to reduce the risk.

The current Homeland Security Authorization Bill for the Department of Homeland Security addresses the issue of risk indirectly in Section 331, which is summarized below:

> Subtitle D: Critical Infrastructure Prioritization - (Sec. 331) Directs the Secretary, within 90 days of enactment of this Act, to complete prioritization of the Nation's critical infrastructure according to the following criteria: (1) the threat of terrorist attack; (2) the likelihood that an attack would destroy or significantly disrupt such infrastructure; and (3) the likelihood that an attack would result in substantial numbers of deaths and serious bodily injuries, a substantial adverse economic impact, or a substantial adverse impact on national security.[37]

This type of analysis provides a more accurate means to prioritize facilities for protection and provides a means to determine what risk is acceptable, knowing we cannot protect everything. However, the term “substantial” must be defined (acceptable risk level) before the requirement can be emplaced.

No prioritization of critical infrastructure. Once risk levels are established and critical infrastructure vulnerabilities are measured against an established risk level, prioritization of the

assets can occur and resources allocated to establish baseline or greater levels of protection as required. Our current policy for the physical protection of critical infrastructure is not effective because it fails to prioritize assets or define the level of protection we should strive to attain. Recognizing that not everything can be protected, a CRS report noted:

> However, it is not practical to try ands protect all of these assets to the same degree. So how will priorities be set and protective measures allocated? According to the National Strategy for Homeland Security, a consistent methodology will be developed and applied to focus the federal government's efforts. The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets makes mention of developing a uniform methodology for identifying facilities, systems and functions with national-level criticality to help establish federal, state, local, and private sector protection priorities. Such a methodology has not yet been articulated. Nor has a methodology been described for setting priorities.[38]

The NIPP uses as one of its steps in prioritization, "identification of priorities, based on overall reduction in risk relative to overall costs."[39] This type of methodology, where priorities are determined by cost and not by criticality, is flawed. Prioritization should be conducted as a resource independent action.

Lack of Responsibility. DHS has lead agency responsibility for protecting our critical infrastructure. Within DHS, the Undersecretary for Information Analysis and Infrastructure Protection and the IA/IP Directorate are responsible for the implementation of the critical infrastructure protection program. However, DHS has assigned Sector-Specific Agencies (SSAs) for each of the thirteen sectors. The interim NIPP defines the DHS role as "establishes uniform policies and approaches for protection activities, and tracks performance and progress in program Implementation," while the role of the SSAs is to "provide the subject matter and industry-specific expertise and relationships to ensure infrastructure protection within the specific sectors."[40] The SSA concept dates back to PDD-63, and does not appear to have evolved with the creation of the DHS. The leadership role given the Undersecretary and IA/IP is not strong enough, and must be expanded beyond one of coordinating, tracking performance, etc., to one of overall responsibility for the program. If the IA/IP is not organized to perform this function, consideration should be given to creating the position of Undersecretary of Protection and Preparedness.[41]

Private sector not integrated. With over 85% of the U.S. critical infrastructure being private or state owned, the impact of making improvements for the sake of protection must be accounted for.

> America's open and technologically complex society includes a wide array of critical infrastructure and key resources that are potential terrorist targets. The

> majority of these are owned and operated by the private sector and State or local governments. These critical infrastructures and key resources are both physical and cyber-based and span all sectors of the economy. [42]

Private industry has to contend with rising insurance costs if a facility is on the critical infrastructure list, and the cost of making improvements is a cost which can not be passed on to the consumer in a competitive market. The federal government must establish a system that requires compliance.

Protection levels ultimately affect the economic bottom line of the individual companies. The acknowledgement that a facility is a potential terrorist target may also affect the facility's insurability, even after protective measures are emplaced. An American Bar Association study noted, "The private sector may be more deliberate, considering the implication of a critical infrastructure program not simply for its net effect on security, but for its net effect on the bottom line."[43] This does not absolve the government from not enforcing the rules it has made. In testimony before the Subcommittee on Infrastructure and Border Security, Peter Orszag of the Brookings Institute made the following comment:

> In homeland security, private markets do not automatically produce the best result. We must therefore alter the structure of incentives so that market forces are directed toward reducing the costs of providing a given level of security for the nation, instead of providing a lower level of security than is warranted. Given the significance of the private sector in homeland security settings, structuring incentives properly is critical.[44]

Orszag went on to explain why private industry cannot be counted on to protect CI: [45]

> Private markets by themselves do not generate sufficient incentives for homeland security for seven reasons:
>
> 1. Private markets will undertake less investment in security than would be socially desirable.
>
> 2. The costs of allowing terrorists to obtain access to highly explosive materials, chemicals, and biological pathogens even if they are stored in private facilities are generally not borne by the facilities themselves; the attacks that use the materials could occur elsewhere. Such a specific negative externality provides a compelling rationale for government intervention.
>
> 3. Contamination effects arise when a catastrophic risk faced by one firm is determined in part by the behavior of others, and the behavior of these others affects the incentives of the first firm to reduce its exposure to the risk... The problem in these settings is that the risk to any member of a network depends not only on its own security precautions but also on those taken by others.
>
> 4. A fourth potential motivation for government intervention involves information – in particular, the cost and difficulty of accurately evaluating security measures.

5. The fifth justification for government intervention is that corporate and individual financial exposures to the losses from a major terrorist attack are inherently limited by the bankruptcy laws.

6. The sixth justification for government intervention is that the private sector may expect the government to bail it out should a terrorist attack occur.

7. The final justification for government intervention involves incomplete markets. The most relevant examples involve imperfections in capital and insurance markets. For example, if insurance firms are unable to obtain reinsurance coverage for terrorism risks (that is, if primary insurers are not able to transfer some of the risk from terrorism costs to other insurance firms in the reinsurance market), some government involvement may be warranted. In addition, certain types of activities may require large-scale coordination, which may be possible but difficult to achieve without governmental intervention.

Lack of information sharing. Essentially, there are two categories of information sharing – first, there must be a system to share information about threats and vulnerabilities; second, there must be a system to share information on protecting CI. Both categories were addressed by Congress in the Critical Infrastructure Information Act (CIIA) of 2002:

> The CIIA was enacted, in part, to respond to the need of the federal government and owners and operators of the nation's critical infrastructures to share information on vulnerabilities and threats, and to promote information sharing between the private and public sectors in order to protect critical assets."[46]

Certain exemptions to the Freedom of Information Act were also enacted to encourage the private sector to voluntarily provide proprietary information to DHS with the knowledge the information was safe from its competitors. Despite these guarantees, information is not freely forthcoming. The GAO found in their report that DHS and the IAIP have made little progress in establishing information sharing systems within the government and the private sector.[47]

> But the stark reality is, compliance is currently voluntary. Unless and until there is a legislative mandate – and extensive funding to support such requirements – it's unlikely that all private-sector organizations will voluntarily take the drastic measures needed. [48]

Lack of accountability for combating terrorism funds. Resources are not adequately allocated to protect those facilities that are truly critical. Unfortunately, our policy of an active, layered defense has as much a horizontal component as well as a vertical dimension. In other words, we attempt to protect too much instead of focusing scarce resources on critical infrastructure. Again, a lack of understanding of the threat, a lack of prioritization, and a lack of a clearly defined definition of CI leads us to spend scarce resources where not needed. The chart below shows how Congress has allocated money since 2002 for critical infrastructure

protection. Unfortunately, the level of protection we have obtained for this expenditure is relatively unknown.

	FY 2002	FY 2003	FY 2004	FY 2005 (Estimated)	FY 2006 (Requested)
Dollars (in millions) allocated by gross budget authority	$9,944.1 / 30%	$13281.7 / 31%	$12,281.7 / 30%	$14,940.2 / 32%	$15632.5 / 31%
Dept of HLS	$1,163.7	$1,990.0	$2128.3	$2585.9	$2820.0
DOD	$4784.0	$8124.0	$6543.8	$7916.9	$8700.8
Dept of Agriculture	$412.3	$60.5	$36.8	$150.6	$129.3
Dept of Energy	$1088.9	$1203.4	$1256.3	$1456.1	$1481.0
Dept of Transportation	$136.3	$128.1	$180.1	$137.0	$141.2
USACE – Civil Works	$100.0	$75.0	$101.5	$88.0	$71.0

Gross Budget Authority for Protecting Critical Infrastructure and Key Assets for Selected U.S. Government Agencies[49]

Table 2.

In January 2006, GAO released a report that examined how money allocated for combating terrorism is spent. The report clearly identified that money allocated by the Congress for combating terrorism is not adequately managed:

> Although OMB's analysis of homeland security funding in the Analytical Perspectives of the President's budget satisfies the current legal requirements under the Homeland Security Act of 2002, it does not provide a complete accounting of all funds allocated to combating terrorism activities.[50]

The report also went on to say that:

> Much of the funding for combating terrorism activities is embedded within appropriation accounts that finance programs that are not primarily homeland security or overseas combating terrorism related. This makes it difficult to identify activities and track funding without such an analysis.[51]

In a similar 2002 report, GAO made the recommendations shown below, which they still believe to be applicable:[52]

- We recommended that OMB require agencies to provide information on obligations in the database used by OMB to produce the President's annual budget request—and that OMB should include obligations as reported in this database in its annual report on combating terrorism.
- That OMB direct relevant departments to develop or enhance combating terrorism performance goals and measures.
- Include national-level and federal governmentwide (sic) combating terrorism performance measures as a supplement to existing strategies and their future revisions

Accountability of funds and level of protection we are purchasing must be managed more efficiently.

Recommendations

The current U.S. policy and the application of that policy can probably best be described as uncoordinated. U.S. policy must be changed if we are to protect our critical infrastructure, and the execution of the new policy must be centralized under one agency. The protection of critical infrastructure should be more than a stand alone plan in support of the National Security Strategy and the National Strategy for Combating Terrorism; it should be an integral component of our active layered defense. Information about these facilities must also be protected from the public domain so as not to enable enemy reconnaissance. The National Strategy for the Physical Protection of CI/KA has it right, but DHS must take the lead.

> It is incumbent in the planning and resource allocation process that federal, state, and local governments and private-sector stakeholders work together to:
>
> - Define clearly their critical infrastructure and key asset protection objectives;
> - Develop a business case for action to justify increased security investments;
> - Establish security baselines, standards and guidelines; and identify potential incentives for security related activities where they do not exist in the marketplace.[53]

Alane Kochems, writing for the Heritage Foundation, recommends three critical tasks that must be addressed before an effective CI protection program can be implemented:[54]

1. The Department of Homeland Security (DHS) should be reorganized to include and Undersecretary of Protection and Preparedness;
2. Congress and the Administration should remove roadblocks to creating a risk-based system that engages the private sector; and
3. The DHS should create effective means for sharing information among federal and state governments, the private sector, and other entities.

The changes recommended by the Heritage Foundation only scratch the surface. Much more must be done in order for us to have an effective program in place.

Redefine CIKA. A better definition for critical infrastructure must be provided so that we are protecting those assets which are truly critical.

> The definition of critical assets must continue to be refined by the private sectors that operate those critical systems and components, with the assistance and encouragement of the DHS in recognition of its lead role.[55]

If the definition is not changed, then the *application* of that definition must be resident in one in one office within DHS, so that there is an executive agent managing the CIP program.

Provide a standardized method to assess vulnerability and risk . The method by which vulnerability is assessed must be codified in one document so there is a common baseline for all agencies to use when evaluating facilities. Risk levels must also be established, so that the impact of terrorist attacks and their potential destruction can be gauged. A baseline level of protection must be mandated, with the expectation that all critical infrastructure will achieve that baseline within a given period. Where the risk is too high once the baseline is in place, additional protective measures can be applied.

Establish a baseline level of protection, and enforce it. Our policy must establish what we can afford to do, but also what we can *not afford to not protect*. A baseline level for protection must be established, so that facilities competing for scarce resources are presenting their separate cases equally to allow a priority list to be established. The methodology used to farm out the responsibility for the protection of critical infrastructure will not work unless the baselines identified above are included in policy. However, a single agency (DHS) should be responsible for the ultimate prioritization, tracking, and execution of the system. Economic incentives must be developed for privately-owned critical infrastructure to build in redundancies and protect critical nodes.

Enforce current policy. DHS must take the leading role in identifying and tracking critical infrastructure and prioritizing the effort to protect it. Existing laws and policy must be enforced. An office or individual must be clearly designated for policy implementation. DHS should consider creating the position of Undersecretary of Protection and Preparedness. It is not a matter of a policy shortfall, it is an issue of establishing systems and responsibility to implement existing policy. The goal must be creating hard targets that deter acts of terrorism, but still allow access when appropriate. The Congress should put tooth into the current policy, to include line item appropriations where required to complete assessments and protection, and fines, government grants, and limits on insurance liability costs. The rules for accountability of funds must also be changes so that we know where our money goes and what it buys for us.

Prioritize assets and allocate resources appropriately. Once CI/KR is adequately defined and responsibility for implementation is assigned, prioritization and resource allocation will begin to take shape. As stated in HSPD-7:

> Federal departments and agencies will identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. Federal departments and agencies will work with State and local government and the private sector to accomplish this objective.[56]

The nation cannot afford to expend scarce resources on protecting infrastructure and facilities that have a very low probability of being attacked, and if attacked, the effects can be mitigated rather quickly. We must also look at a systems approach to securing infrastructure with emphasis on protecting those nodes most vulnerable and whose destruction or disruption will cause catastrophic consequences. Concurrent with the systems approach, redundancies must be identified, and when not present, programmed for inclusion in our protection process. There must also be a means provided to prioritize those critical infrastructure nodes so that money can be appropriated correctly.

Develop incentives for public critical infrastructure to participate . In his testimony before Testimony before the Subcommittee on Infrastructure and Border Security of the House Select Committee on Homeland Security, Peter Orszag listed three ways the government could intervene to force the private sector to protect critical infrastructure: [57]

- Impose direct regulation
- Require insurance
- Provide a subsidy for anti-terrorism measures

Rather than allow private industry to participate on a voluntary basis, CI must be managed by the federal government. DHS should go to Congress for a new version of the Critical Infrastructure Information Act that mandates participation by private industry for those assets which are CI/KR, and that also provides adequate protection for proprietary information.

Conclusion

The United States, as does any developed country, has a tremendous amount of infrastructure, not all of which can be protected from terrorist attack. The DHS must work with Congress to arrive at a better method to determine what is critical, prioritize that infrastructure which meets the new criteria, and then apply the necessary resources to protect it from attack. We need a system that includes timelines, objectives, milestones, and performance measures to gage compliance and preparedness.

Private industry must be held accountable to protect their critical infrastructure to at least a baseline level that will effectively dissuade terrorists from attacking that target. Congress must make participation in the critical infrastructure program mandatory, applying tax breaks where applicable.

Finally, we must as a nation, do more to educate our people about the threat so that we can prevent mass hysteria and concern from driving us to bad decisions and misallocation of

resources. The U.S. will always be a terrorist target, but an understanding of the threat will help ensure we allocate scarce resources wisely so that we can minimize the effect of any attack.

Endnotes

[1] George W. Bush, *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* (Washington, D.C.: The White House, February 2003), vii.

[2] Ibid., 8.

[3] Department of Homeland Security, *The Interim National Infrastructure Protection Plan* (Washington, D.C.: Department of Homeland Security, February 2005), 1.

[4] Keith B. Payne, "Post-Cold War Deterrence and Missile Defense," *Orbis*, Spring 1995, 203; quoted in Philip L. Ritcheson, "Proliferation: Scope, Prospects, and Implications," *Naval War College Review*, Summer 1997, 530.

[5] United States Army War College, "Lesson 15: Terrorism and Religious Violence," *National Security Policy and Strategy Course Directive*, (Carlilse Barracks, PA: United States Army War College), 69.

[6] *USA Patriot Act of 2001, United States Code,* section 1016(e) (2001).

[7] Bruce Don and David Mussington, "Protecting Critical Infrastructure," available from http://www.rand.org/publications/randreview/issues/rr.08.02/infrastructure.html; Internet; Accessed 8 Sept 05

[8] John Moteff, *Critical Infrastructures: Background, Policy, and Implementation* (Washington, D.C.: Congressional Research Service, updated July 12, 2005), 13

[9] William J. Clinton, *Presidential Directive – 63* (Washington, D.C.: The White House, May 22, 1998), 1.

[10] Clinton. 6.

[11] Bush., 17.

[12] Ibid., 6.

[13] Ibid., 7.

[14] Department of Homeland Security, *The Interim National Infrastructure Protection Plan* , 3. The Interim NIPP states this definition comes from the Homeland Security Act.

[15] Bush, 2-3.

[16] Department of Homeland Security, *The Interim National Infrastructure Protection Plan,* 7-8.

[17] Tom Ridge, "Department of Homeland Security FY 2005 Homeland Security Grant Program – Solicitation of Applications from State Organizations," available from http://www.ojp.usdoj.gov/dp/docs/fy05hsgp.pdf#search='fy%202005%20Homeland%20Security%20Grant%20Program'; Internet; accessed 4 Oct 2005. 2.

[18] Ibid., 4. Those priorities are:

1. National Incident management System adoption and implementation
2. Homeland Security Presidential Directive -8 initiatives adoption and implementation
3. National Response Plan
4. Critical Infrastructure Protection
5. Other Planning Activities
6. Operational Activities
7. Other Exercise Activities
8. Other Training Activities
9. Other Equipment Needs

[19] U.S. General Accounting Office, *Combating Terrorism: Determining and Reporting Federal Funding Data* (Washington, D.C.: U.S. General Accounting Office, January 2006). This is the overall theme of the GAO Report. The report does not construe that money is inappropriately handled, just that there is no accountability to show what we, as a Nation, are buying for the money given the agencies.

[20] Ibid., 8

[21] Department of Homeland Security, *The Interim National Infrastructure Protection Plan*, 9.

[22] Author unknown. "The Safety and Security of Critical Infrastructure," available from http://faculty.ncwc.edu/TOCXonnor/431/431lect06.htm; Internet; Accessed 25 Aug 05

[23] Alane Kochems, "Who's on First? A Strategy for Protecting Critical Infrastructure," *Backgrounder* #1851 (May 9, 2005):available from http://www.heritage.org/Research/HomelandDefense/bg1851.cfm; Internet; accessed October 30, 2005. 3.

[24] John Moteff, *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities, and Consequences* (Washington, D.C.: Congressional Research Service, September 2, 2004), 5.

[25] Ibid., 22-23.

[26] The Buffer Zone Protection Program provides both funding and coordination in bringing federal, state and local levels of government, law enforcement and the private sector together to create Buffer Zone Plans to reduce vulnerabilities in areas surrounding critical infrastructure and key resources. Department of Homeland Security Webpage, "Department of Homeland Security Announces $91.3 Million in Buffer Zone Protection Program Grants," March 2, 2005, Available at http://www.dhs.gov/dhspublic/display?content=4380, Internet, Accessed 26 Feb 2006.

[27] Ibid., 17.

[28] Department of Homeland Security, *The Interim National Infrastructure Protection Plan*, 1.

[29] Moteff, *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities, and Consequences*, 8.

[30] Ibid., 7.

[31] U.S. General Accounting Office, *Combating Terrorism: Determining and Reporting Federal Funding Data,* 24

[32] Kochems, 2.

[33] John Moteff, *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities, and Consequences* (Washington, D.C.: Congressional Research Service, September 2, 2004), 21

[34] Moteff, *Critical Infrastructures: Background, Policy, and Implementation*, 5.

[35] Ibid., 10.

[36] Moteff, *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities, and Consequences*, 10.

[37] House of Representatives, H.R. 1817, 109th Congress, 1st Session, Department of Homeland Security Authorization Act for Fiscal Year 2006; Available at http://www.washingtonwatchdog.org/rtk/documents/cong_bills/109/h/h109_1817eh.html; Internet; Accessed 5 March 2006.

[38] John D. Moteff, *Critical Infrastructures: Background, Policy, and Implementation,* 8.

[39] Department of Homeland Security, *The Interim National Infrastructure Protection Plan*, 19.

[40] Department of Homeland Security, *The Interim National Infrastructure Protection Plan*, 4.

[41] Kochems, 4.

[42] George W. Bush, *Homeland Security Presidential Directive – 7: Critical Infrastructure Identification, Prioritization, and Protection* (Washington, D.C.: The White House, December 17, 2003).

[43] Steven Roberts, "Tips and Trends for Homeland Security and Critical Infrastructure Protection," *Journal of Homeland Security and Emergency Management;* available from http://www.bepress.com/jhsem/vol1/iss4/; Internet; accessed 27 December 2005.

[44] Peter R. Orszag, Critical Infrastructure Protection and the Private Sector: The Crucial Role of Incentives, Testimony before the Subcommittee on Cybersecurity, Science, and Research & Development and the Subcommittee on Infrastructure and Border Security House Select Committee on Homeland Security, September 4, 2003, available at http://www. brookings.edu/views/testimony/orszag/20030904.pdf; Internet; accessed 26 Feb.

[45] Ibid.

[46] Gina Marie Stevens , , *Homeland Security Act of 2002: Critical Infrastructure Information Act* (Washington, D.C.: Congressional Research Service, February 28, 2003), 3.

[47] U.S. General Accounting Office, *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors (*Washington, D.C.: U.S. General Accounting Office, July 2004), 9. "The federal government and the private sector should share information on incidents, threats, and vulnerabilities."

[48] Patricia McAnally, "Can We Count on Critical Infrastrucutres ?" available from http:// www. availability.sungard.com/NR/rdonlyres/0669AD60-F634-458E-A475-4E5892F2C041 /0/CTalk_CanWeCountonCritical.pdf#search='patricia%20mcanally%20can%20we%20count'; Internet, accessed 15 January 2006.

[49] U.S. General Accounting Office, *Combating Terrorism: Determining and Reporting Federal Funding Data,* 54-62.

[50] Ibid., 26

[51] Ibid., 3

[52] Ibid., 20-22

[53] Bush, *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*, 23.

[54] Kochems , 1.

[55] ISAC Council, "Homeland Security Presidential Directive – 7: Issues and Metrics," January 31, 2004; Available from http://www.isaccouncil.org/pub/HSPD7_Issues and_ Metrics_013104.pdf#search='isac%20council%20white%20paper%20homeland%20security%2 0presidential%20directive%207'; Internet; Accessed 30 October 2005, 2.

[56] Bush, *Homeland Security Presidential Directive – 7: Critical Infrastructure Identification, Prioritization, and Protection*

[57] Orszag.